In the Claims

This listing of claims replaces all prior versions and listings of the claims in the application.

Please amend the claims as follows:

1. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system comprising:

receiving a proffered biometric sample at a biometric sensor configured on a smartcard;

generating data representing said proffered biometric sample;

using said data representing said proffered biometric sample as a variable in an encryption calculation to secure at least one of user data and transaction data;

verifying said proffered biometric sample; and

~~accessing at least one of a partner file structure and a common file structure stored on a smartcard having an integrated circuit device comprising a common application and a second application, said second application being configured to store travel-related information associated with a cardholder;~~

~~said second application comprising said common file structure and said partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to a file in said common file structure;~~

~~verifying whether a smartcard transaction is in compliance with a preset transaction limitation; and~~

facilitating authorization of ~~said~~ a smartcard transaction.

2. (Previously Presented) The method of claim 1, further comprising registering said proffered biometric sample with an authorized sample receiver.

3. (Previously Presented) The method of claim 2, wherein said step of registering includes at least one of: contacting said authorized sample receiver, proffering said proffered biometric sample to said authorized sample receiver, associating said proffered biometric sample with user information, verifying said proffered biometric sample, and storing said proffered biometric sample upon verification.

4. (Previously Presented) The method of claim 1, wherein said step of receiving said proffered biometric further includes at least one of: storing, comparing, and verifying said proffered biometric sample.

5. (Previously Presented) The method of claim 1, wherein said step of receiving said proffered biometric sample further includes processing database information, wherein said database information is contained in at least one of said smartcard, a smartcard reader, said biometric sensor, a remote server, a merchant server and said smartcard system.

6. (Previously Presented) The method of claim 1, wherein said step of receiving said proffered biometric sample further includes comparing said proffered biometric sample with a stored biometric sample.

7. (Previously Presented) The method of claim 6, wherein said step of comparing includes comparing said proffered biometric sample to said stored biometric sample by using at least one of a third-party security vendor device and a local CPU.

8. (Previously Presented) The method of claim 1, wherein said step of receiving said proffered biometric sample further includes at least one of detecting, processing and storing a second proffered biometric sample.

9. (Previously Presented) The method of claim 1, wherein said step of verifying said proffered biometric sample further includes using a secondary security procedure, said secondary security procedure including sending a signal to notify that a requested transaction would violate an established rule for said smartcard.

10. (Previously Presented) The method of claim 1, wherein said step of receiving said proffered biometric sample at said biometric sensor includes receiving said proffered biometric sample at at least one of: a retinal scan sensor, an iris scan sensor, a fingerprint sensor, a hand print sensor, a hand geometry sensor, a voice print sensor, a vascular sensor, a facial sensor, an

ear sensor, a signature sensor, a keystroke sensor, an olfactory sensor, an auditory emissions sensor, and a DNA sensor.

11. (Currently Amended) The method of claim 1, ~~wherein said~~ further comprising verifying whether a smartcard transaction is in compliance with a preset transaction limitation ~~is~~ associated with at least one of a: charge card account, credit card account, debit card account, savings account, private label account and loyalty point account.

12. (Cancelled)

13. (Currently Amended) The method of claim 1, ~~wherein said~~ further comprising verifying whether a smartcard transaction is in compliance with a preset transaction limitation comprising ~~comprises~~ at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

14. (Currently Amended) The method of claim 1, further comprising requiring a second proffered biometric sample to override ~~said~~ a preset transaction limitation.

15. (Currently Amended) The method of claim 1 ~~6~~, further comprising accessing at least one of a partner file structure and a common file structure stored on a smartcard having an integrated circuit device comprising a common application and a second application, said second application being configured to store travel-related information associated with a cardholder;

said second application comprising said common file structure and said partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to a file in said common file structure ~~wherein said stored biometric sample is stored by one of a third-party biometric security vendor and a governmental agency~~.

16. (Previously Presented) The method of claim 15 ~~1~~, further comprising accessing card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel in said first partner file structure.

17. (Previously Presented) The method of claim 16, further comprising updating said card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel in said first partner file structure.

18. (Cancelled)

19. (New) The method of claim 1, further comprising using said data representing said proffered biometric sample as at least one of a private key, a public key, and a message authentication code to facilitate transaction security measures.

20. (New) The method of claim 1, further comprising using said data representing said proffered biometric sample in generating a message authentication code and as at least one of a private key and a public key.

21. (New) The method of claim 1, further comprising using said data representing said proffered biometric sample to facilitate substantially simultaneous access to goods and initiation of authentication for a subsequent purchase of said goods.

22. (New) A method for facilitating biometric security in a smartcard transaction system comprising:

receiving a proffered biometric sample at a biometric sensor configured on a smartcard;

generating data representing said proffered biometric sample;

using said data representing said proffered biometric sample as least one of a variable in an encryption calculation, a private key, a public key, and a message authentication code to secure at least one of user data and transaction data;

verifying said proffered biometric sample; and

facilitating authorization of a smartcard transaction.